Notes on Completion: Please refer to the appropriate NIA Governance Document to assist in the completion of this form. The full completed submission should not exceed 6 pages in total.

NIA Project Registration and PEA Document

Date of Submission

Sep 2018

Project Reference Number

NIA_NGTO020

Project Registration

Project Title

IEC 61850 Cyber Resilient Electric Substation Technologies

Project Reference Number

NIA_NGTO020

Project Licensee(s)

National Grid Electricity Transmission

Project Start

November 2018

Project Duration

2 years and 9 months

Nominated Project Contact(s)

Linwei Chen

Project Budget

£404,000.00

Summary

Digital substation technologies have the potential to deliver great benefits to utilities and their customers. They can enable a more efficient, automated and less risky engineering process, simplified installation, commissioning and eventually replacement, requiring shorter outages and significantly fewer resources. To fully explore these benefits, National Grid has previously carried out two research projects which have delivered a standard Architecture for Substation Secondary Systems (AS3), including a configuration guideline for digital substation solutions based on the IEC61850 suite of standards.

Building on this work, the Virtual Site Acceptance Testing and Training (VSATT) project has developed an off-grid test facility implementing the AS3 architecture and configuration guidelines. The VSATT project demonstrated a good level of interoperability between suppliers and delivered a testing and commissioning strategy for digital substation solutions. Whilst this research work has significantly improved our readiness to deploy this technology and deliver the benefits, security and resilience issues have arisen that require further work. This project will investigate cyber vulnerabilities particularly for digital solutions, and it will develop defence/recovery methods to improve resilience.

Nominated Contact Email Address(es)

box.NG.ETInnovation@nationalgrid.com

Problem Being Solved

Digital substation technologies have the potential to deliver great benefits to utilities and their customers. They can enable a more efficient, automated and less risky engineering process, simplified installation, commissioning and eventually replacement, requiring shorter outages and significantly fewer resources. To fully explore these benefits, National Grid has previously carried out two research projects which have delivered a standard Architecture for Substation Secondary Systems (AS3), including a configuration guideline for digital substation solutions based on the IEC61850 suite of standards.

Building on this work, the Virtual Site Acceptance Testing and Training (VSATT) project has developed an off-grid test facility implementing the AS3 architecture and configuration guidelines. The VSATT project demonstrated a good level of interoperability between suppliers, whilst highlighting a few areas where suppliers need to make further progress. The VSATT project also delivered a testing and commissioning strategy for digital substation solutions and the learning was incorporated in the updated configuration guidance and merging unit specification. Whilst this research work has significantly improved our readiness to deploy this technology and deliver the benefits, some additional issues have arisen that require further work:

Cyber security and resilience

- Recent events have highlighted the risk related to cyber security and this concerns in particular digital protection, automation and control systems.

- Overreliance on GPS as a time source can lead to reduced network security and therefore to build resilience for time synchronisation is of vital importance to future digital substation roll out.

- The behaviour of digital substation solutions in response to abnormal network traffic resulting from equipment failure or unexpected messages from cyber-attack on the process bus or station bus is unknown.

Station-wide functions and commissioning with a mix of analogue and digital technologies

- Roll out of digital substation solutions will most likely require a bay-by-bay approach. This will lead to substations with mixed, digital and conventional bays. The feasibility and challenges associated with this in particular where station-wide functions such as Automatic Tap Changer Control (ATCC), Synchronising, Interlocking, Busbar Protection etc. are concerned require further study.

Bespoke I/O interfaces to primary equipment

- Various types of interfaces between secondary systems and primary plant have been used by National Grid and other utilities. A significant amount of outage time is required to interface the secondary to the primary equipment.

Method(s)

To address the above problems, the following research and development work is proposed:

- Design and implement cyber security testing capability into the existing VSATT platform. This will require a suite of software tools running on several devices that can be connected at process and station bus levels. It will enable the assessment of a number of commercial cyber security tools and investigations into the vulnerability of equipment/network in a virtual substation environment.
- Develop and test new methods of managing cyber security and improving resilience for IEC 61850 based networks, e.g. collaborative defence mechanisms, etc.

- Evaluate and trial innovative methods related to recovery from a cyber-attack or equipment failure, e.g. hot standby bay strategy, and self-healing systems based on Software-Defined Networking technology.
- Extend the VSATT platform by installing a traffic generator and standard physical I/O interfaces between the simulated primary plant and merging units. This will allow testing the impacts of delayed, missing or modified network traffic in digital P&C systems and assessing the influence of standardised I/O interfaces on system outage time.

Scope

The AS3 and VSATT projects have demonstrated the viability of implementing digital substation solutions and have validated the interoperability between solutions from several vendors. However, the increase in cyber risk and concern about the resilience of digital P&C solutions has led to a need to better understand how the IEDs now being used in National Grid substations might be attacked and the extent of their vulnerability. The scope of this project can be divided into the following parts.

Cyber security and resilience of IEC 61850 based substation solutions

- Review and report on literature, including cyber security issues and new emerging cyber-attack detection/defence technologies in substation protection, automation and control systems.

- Trial different Intrusion Detection Systems (IDS) on the VSATT platform to identify vulnerabilities of AS3 based digital substations.
- Develop and demonstrate cyber defence and recovery methods for IEC 61850 based substation protection and control schemes.
- Develop a specification and/or best practice guidance for cyber-resilient digital substation solutions considering in particular how relevant international cyber security standards should be implemented and identify any gaps not currently covered by international standards.

Station-wide functions and commissioning for hybrid substations

- Test and demonstrate AS3 bay solutions and station-wide functions with a mix of analogue and digital technologies, including Bus Bar Protection (BBP), synchronising and interlocking.

Standardised I/O interface to primary equipment

- Test and demonstrate the impact of a standardised quick-release I/O interface to primary equipment on the IEC 61850 bay solution outage time when replacing and testing the secondary system using the VSATT platform.

The project will comprise a number of work streams, including the development of a suitable cyber detection tool as well as protection and control resiliency methods. The testing in this project will aim to answer, but not be limited to, the following questions.

- What is the level of cyber security risk and equipment vulnerability for digital bay solutions based on the AS3 architecture?
- Can these risks and vulnerabilities be addressed and managed?
- What is the most suitable cyber resiliency technology going forwards?

Objective(s)

The project aims to address the cyber security and secondary system resiliency issues in order to facilitate the application of AS3 digital substation architecture based designs on the transmission network. The main enabling factor is to implement station-wide functions with a mix of analogue and digital technologies as well as cyber security testing capability into the existing VSATT platform to achieve the following:

- Test and demonstrate station-wide functions and commissioning, testing and maintenance strategies with mixed analogue and digital technologies and enable site roll out.
- Test and demonstrate protection and control, cyber resilient technologies in the event of equipment failure or virus intrusion from any test set, laptop or memory stick for software update during commissioning, maintenance and live equipment testing.
- Reduce the overall technical and commercial risks associated with secondary systems and drive customer value as a result of:
- fast response to cyber-attacks with suitable intrusion detection tools,
- improved resiliency of digital P&C solutions

Consumer Vulnerability Impact Assessment (RIIO-2 Projects Only)

n/a

Success Criteria

If successful, this project will provide the following key outcomes:

- A review of the current state of the art and evolving technologies in the literature relating to cyber security issues and defence mechanisms for substation protection automation and control systems as well as the corresponding tools.

- Test evidence on the performance of cyber security tools using the VSATT platform and a study of the cyber risks associated with IEC 61850 traffic.

- Investigation and development of cyber resilient Protection and Control solutions, for AS3 based digital substations and application guidance for cyber security in substation secondary systems.

- Feasibility study and demonstration of the integration of digital bays into conventional substations and their impact on station-wide functions, in particular Synchronising, Interlocking and Busbar Protection.
- Analysis of the impacts of a standard physical I/O interfaces (between primary plants and merging units) on the outage time during equipment commissioning, testing and maintenance.

Project Partners and External Funding

N/A

Potential for New Learning

This project will further investigate the benefits, technical challenges and cyber vulnerabilities of digital substation technologies. In particular, the requirements for improving cyber security and resilience of AS3 based secondary systems will be better understood.

Scale of Project

The project will carry out off-grid tests based on a previously developed protection test facility – VSATT. The platform has been established with four digital feeder bay solutions and two substation Human Machine Interfaces (HMIs) from different vendors. This will simulate a comprehensive substation secondary system and enable the project team to demonstrate proof of concept.

Technology Readiness at Start

TRL2 Invention and Research

Technology Readiness at End

TRL4 Bench Scale Research

Geographical Area

The research study will be predominantly laboratory and desktop based. The testing will be carried out on the VSATT platform at Manchester.

Revenue Allowed for the RIIO Settlement

None

Indicative Total NIA Project Expenditure

£404,000

Project Eligibility Assessment Part 1

There are slightly differing requirements for RIIO-1 and RIIO-2 NIA projects. This is noted in each case, with the requirement numbers listed for both where they differ (shown as RIIO-2 / RIIO-1).

Requirement 1

Facilitate the energy system transition and/or benefit consumers in vulnerable situations (Please complete sections 3.1.1 and 3.1.2 for RIIO-2 projects only)

Please answer **at least one** of the following:

How the Project has the potential to facilitate the energy system transition:

n/a

How the Project has potential to benefit consumer in vulnerable situations:

n/a

Requirement 2 / 2b

Has the potential to deliver net benefits to consumers

Project must have the potential to deliver a Solution that delivers a net benefit to consumers of the Gas Transporter and/or Electricity Transmission or Electricity Distribution licensee, as the context requires. This could include delivering a Solution at a lower cost than the most efficient Method currently in use on the GB Gas Transportation System, the Gas Transporter's and/or Electricity Transmission or Electricity Distribution licensee's network, or wider benefits, such as social or environmental.

Please provide an estimate of the saving if the Problem is solved (RIIO-1 projects only)

This research project aims to identify the potential cyber security issues for IEC 61850 networks and to improve system resilience by investigating various intrusion detection systems and innovative methods related to recovery from a cyber-attack. The outcomes will increase the confidence of power utilities to deploy digital bays or substations on site, resulting in less outage time compared to the conventional bay solutions. Managing and reducing the cyber risk is a key enabler that allows stakeholders a secure rollout of digital substation technology and access to the associated benefits. It also reduces the cost associated with the risk to the transmission system as a result of in-service equipment. Financial benefits are expected to be primarily derived from a reduction in costs associated with the prevention of a cyber-attack. The savings will be estimated based on the specific outcomes generated from the project.

Please provide a calculation of the expected benefits the Solution

Not applicable – this is primarily a research project.

Please provide an estimate of how replicable the Method is across GB

The method can be applied to all substation configurations in GB. However, the principle is only valid for substations where IEC 61850 will be considered.

Please provide an outline of the costs of rolling out the Method across GB.

Roll out with new projects – no retrofit envisaged at this stage.

Requirement 3 / 1

Involve Research, Development or Demonstration

A RIIO-1 NIA Project must have the potential to have a Direct Impact on a Network Licensee's network or the operations of the System Operator and involve the Research, Development, or Demonstration of at least one of the following (please tick which applies):

☑ A specific piece of new (i.e. unproven in GB, or where a method has been trialled outside GB the Network Licensee must justify repeating it as part of a project) equipment (including control and communications system software).

□ A specific novel arrangement or application of existing licensee equipment (including control and/or communications systems and/or software)

☑ A specific novel operational practice directly related to the operation of the Network Licensees system

□ A specific novel commercial arrangement

RIIO-2 Projects

□ A specific piece of new equipment (including monitoring, control and communications systems and software)

□ A specific piece of new technology (including analysis and modelling systems or software), in relation to which the Method is unproven

□ A new methodology (including the identification of specific new procedures or techniques used to identify, select, process, and analyse information)

□ A specific novel arrangement or application of existing gas transportation, electricity transmission or electricity distribution equipment, technology or methodology

□ A specific novel operational practice directly related to the operation of the GB Gas Transportation System, electricity transmission or electricity distribution

□ A specific novel commercial arrangement

Specific Requirements 4 / 2a

Please explain how the learning that will be generated could be used by the relevant Network Licensees

Although there has been work carried out on the IEC 61850 substation communication protocol, there is no facility to test cyber security issues of digital substation networks without putting actual substations at risk.
The project will enhance the understanding of the technical and practical viability of digital substation technologies and identify potential opportunities, barriers and areas for further research. Therefore, the findings could benefit other transmission and distribution network operators, in particular configuration guidance for cyber secure digital substation solutions which should enable all relevant stakeholders to improve their level of cyber security. High-level outputs will be shared with the energy industry via a dissemination event, which will be open to licensees

Or, please describe what specific challenge identified in the Network Licensee's innovation strategy that is being addressed by the project (RIIO-1 only)

This project fits within the Managing Assets value area of the Electricity Innovation Strategy.

☑ Has the Potential to Develop Learning That Can be Applied by all Relevant Network Licensees

Is the default IPR position being applied?

☑ Yes

Project Eligibility Assessment Part 2

Not lead to unnecessary duplication

A Project must not lead to unnecessary duplication of any other Project, including but not limited to IFI, LCNF, NIA, NIC or SIF projects already registered, being carried out or completed.

Please demonstrate below that no unnecessary duplication will occur as a result of the Project.

To the best of our knowledge, this work has not been conducted before. This review has included the ENA smart portal, and supply base (including Universities and EPRI). There are a number of similar sounding projects, however, they are examining and testing different aspects, in most cases equipment has been tested individually and the focus has been on testing the security of each individual device. This project will investigate the resilience of digital substations at a larger system level in a multi-vendor substation protection automation and control system including station bus and process bus networks

If applicable, justify why you are undertaking a Project similar to those being carried out by any other Network Licensees.

n/a

Additional Governance And Document Upload

Please identify why the project is innovative and has not been tried before

Although the previous project outcomes have significantly improved our readiness to deploy digital substation technologies, the increasing cyber security concerns require further work. This project is innovative because cyber security of digital substations will be first time investigated at a system level with multi-vendor solutions. The project will shape our understanding of vulnerabilities for IEC 61850 traffic in AS3 based substations and develop a corresponding defence/recovery method to improve resilience.

Relevant Foreground IPR

n/a

Data Access Details

n/a

Please identify why the Network Licensees will not fund the project as apart of it's business and usual activities

The nature of a research programme means it inherently carries a risk that the research may be unsuccessful and/or identify unforeseen barriers to implementation and National Grid is unable to consider the research of this scale as business-as-usual. The NIA funding offers the most appropriate route for the National Grid Electricity Transmission (NGET) to evaluate how IEC 61850 based digital solutions can be adopted into existing/new substations and maintained with high cyber resilience.

Please identify why the project can only be undertaken with the support of the NIA, including reference to the specific risks(e.g. commercial, technical, operational or regulatory) associated with the project

The inherent risk of the project is detailed above and the learning from the project will be directly relevant to all Network Licensees. For this reason, NGET believes this project is appropriately funded through NIA, and material from the project will be available to the general public via the ENA portal.

This project has been approved by a senior member of staff

☑ Yes